

---

## WHAT NEXT FOR NETWORKS AND NETWAR?

---

*David Ronfeldt and John Arquilla*

*Editors' abstract. As with other new modes of conflict, the practice of netwar is ahead of theory. In this concluding chapter, we suggest how the theory of netwar may be improved by drawing upon academic perspectives on networks, especially those devoted to organizational network analysis. Meanwhile, strategists and policymakers in Washington, and elsewhere, have begun to discern the dark side of the network phenomenon, especially among terrorist and criminal organizations. But they still have much work to do to harness the bright side, by formulating strategies that will enable state and civil-society actors to work together better.*

### THE SPREAD OF NETWORK FORMS OF ORGANIZATION

The deep dynamic guiding our analysis is that the information revolution favors the rise of network forms of organization. The network appears to be the next major form of organization—long after tribes, hierarchies, and markets—to come into its own to redefine societies, and in so doing, the nature of conflict and cooperation. As noted in the introductory chapter, the term *netwar* calls attention to the prospect that network-based conflict and crime will be major phenomena in the years ahead. The chapters in this volume provide early evidence for this.

### Changes for the Better

The rise of networks is bringing many changes for the better. Some hold out the promise of reshaping specific sectors of society, as in

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>2001</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2001 to 00-00-2001</b>	
4. TITLE AND SUBTITLE <b>What Next for Networks and Netwars?</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Naval Postgraduate School, Graduate School of Operational and Information Sciences, Department of Defense Analysis, Monterey, CA, 93943</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>In Networks and Netwars: The Future of Terror, Crime, and Militancy (John Arquilla and David Ronfeldt eds.), Santa Monica, CA: RAND, 1993-2003</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>51</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

writings about the promises of “electronic democracy,” “networked corporations,” “global civil society,” and even “network-centric warfare.”<sup>1</sup> Other likely effects are broader and portend the reshaping of societies as a whole, such that writers herald the coming of “the network society,” “the network age,” and even the redefinition of “nations as networks.”<sup>2</sup> In addition, key academic studies of globalization revolve around observations about the growth of global networks and their interconnection with networks at local levels of society.<sup>3</sup> Many writings are speculative, but others, particularly in the business world, are usually quite practical, inquiring into exactly what kinds of network structures and processes work, and which do not.<sup>4</sup>

At a grand theoretical level, age-old ideas about life as a “great chain of being” or as a progression of nested hierarchies are giving way to new ideas that networks are the key to understanding all of life. Here, theorists argue that hierarchies or networks (or markets, for that matter) are mankind’s finest form of organization, and that one or the other design underlies essentially all order in the world. In the social sciences, for example, some key 1960s writings about general systems theory (e.g., Bertalanffy, 1968) and social complexity (e.g., Simon, 1969) took stances lauding the roles of hierarchy in many areas of life. But since the 1970s, and especially in the 1990s, ideas have come slowly to the fore that networks are the crucial design. Thus, it is said that “most real systems are mixtures of hierarchies and networks” (Pagels, 1989, p. 51; also La Porte, 1975), and that “the web of life consists of networks within networks,” not hierarchies (Capra, 1996, p. 35; also

---

<sup>1</sup>The literatures on each of these concepts is, by now, quite large, except for “network-centric warfare,” whose main source is Cebrowski and Garstka (1998). Some writers (e.g., Florini, 2000) prefer the term “transnational civil society” over “global civil society.”

<sup>2</sup>See Kelly (1994) and Lipnack and Stamps (1994) on “the network age,” Castells (1996) and Kumon (1992) on “the network society,” and Dertouzos (1997) on “networks as nations.”

<sup>3</sup>See Held and McGrew (2000), esp. Ch. 2 (excerpted from a 1999 book by David Held, Anthony McGrew, David Goldblatt, and Jonathan Perraton), and Ch. 11 (from a 1997 paper by Michael Mann). Also see Rosenau (1990) and Nye and Donahue (2000).

<sup>4</sup>The *Harvard Business Review* is a fine source of business-oriented references, e.g., Evans and Wurster (1997) and Coyne and Dye (1998), which address banking networks, and Jacques (1990), which provides a classic defense of the importance of hierarchy in corporate structures.

Kelly, 1994). So many advances are under way in the study of complex networks that

In the longer run, network thinking will become essential to all branches of science as we struggle to interpret the data pouring in from neurobiology, genomics, ecology, finance, and the World-Wide Web (Strogatz, 2001, p. 275).

## **The Dark Side**

Most people might hope for the emergence of a new form of organization to be led by “good guys” who do “the right thing” and grow stronger because of it. But history does not support this contention. The cutting edge in the early rise of a new form may be found equally among malcontents, ne’er-do-wells, and clever opportunists eager to take advantage of new ways to maneuver, exploit, and dominate. Many centuries ago, for example, the rise of hierarchical forms of organization, which displaced traditional, consultative, tribal forms, was initially attended, in parts of the world, by the appearance of ferocious chieftains bent on military conquest and of violent secret societies run according to rank—long before the hierarchical form matured through the institutionalization of states, empires, and professional administrative and bureaucratic systems. In like manner, the early spread of the market form, only a few centuries ago, was accompanied by a spawn of usurers, pirates, smugglers, and monopolists, all seeking to elude state controls over their earnings and enterprises.<sup>5</sup>

Why should this pattern not be repeated in an age of networks? There appears to be a subtle, dialectical interplay between the bright and dark sides in the rise of a new form of organization. The bright-side actors may be so deeply embedded in and constrained by a society’s established forms of organization that many have difficulty becoming the early innovators and adopters of a new form. In contrast, nimble bad guys may have a freer, easier time acting as the cutting edge—and reacting to them may be what eventually spurs the good guys to innovate.

---

<sup>5</sup>Adapted from Ronfeldt (1996).

The spread of the network form and its technologies is clearly bringing some new risks and dangers. It can be used to generate threats to freedom and privacy. New methods for surveillance, monitoring, and tracking are being developed; and the uproars over the intelligence systems “Echelon,” “Semantic Forests,” and “Carnivore” manifest what will surely be enduring concerns. Critical national infrastructures for power, telecommunications, and transportation, as well as crucial commercial databases and information systems for finance and health, remain vulnerable to computer hackers and cyberterrorists. Furthermore, a growing “digital divide” between information “haves” and “have-nots” portends a new set of social inequities. All this places new strains on the world’s democracies. Even worse is the possibility that information-age dictatorships will arise in parts of the world, based on the skillful exploitation of the new technologies for purposes of political command and control.

### **Ambivalent Dynamics of Netwar**

As this volume shows, netwar, in all its varieties, is spreading across the conflict spectrum. Instances abound among violent terrorists, ethnonationalists, criminals, and ideological fanatics who are anathema to U.S. security interests and policies. At the same time, many militant yet mainly peaceable social networks are being waged around the world by democratic opponents of authoritarian regimes and by protestors against various risky government and corporate policies—and many of these people may well be agents of positive change, even though in some cases their ideas and actions may seem contrary to particular U.S. interests and policies.

In other words, netwar is an ambivalent mode of conflict—it has a dual nature. While it should not be expected that the dystopian trends associated with the dark side of netwar will prevail in the years ahead, they will surely contend, sometimes bitterly, with the forces of the bright side.

Netwar is not likely to be a passing fancy. As the information revolution spreads and deepens around the world, instances of netwar will cascade across the spectrum of conflict and crime. So will the sophistication and the arsenal of techniques that different groups can mus-

ter. At present, the rise of netwar extends from the fact that the world system is in a turbulent, susceptible transition from the modern era, whose climax was reached at the end of the cold war, to a new era that is yet to be aptly named. Netwar, because of its dependence on networks, is facilitated by the radical increases in global and transnational connectivity, as well as from the growing opportunities for increased connectivity in another sense—the ability of “outsiders” and “insiders” to gain access to each other, and even for insiders to be sequestered within an organization or sector of society.<sup>6</sup> All this means that netwar is not a transitional phenomenon; it will likely be a permanent aspect of the new era.

### **WHEN IS A NETWORK REALLY AN ORGANIZATIONAL NETWORK?<sup>7</sup>**

Netwar rests on the dynamics of networks. Yet, what does the term “network” mean? Discussions about networks are proliferating, and three usages are in play, with clear distinctions rarely drawn among them. One common usage refers to communications grids and circuits—as though networking were a technological phenomenon, such that placing a set of actors (military units, for example) atop a grid would make them a network. This is a limited usage; we have spoken about its pitfalls in this and earlier studies, and thus will not dwell further upon it here.

In two other prominent usages, the term refers either to social networks or to organizational networks (or to a conflation of both). But social and organizational networks are somewhat different organisms. This is what needs discussion here, because the difference is a significant issue for theory and practice, affecting how best to think about the dynamics of netwar. The field of network analysis, writ large, has been dominated by social network analysis, but organizational network analysis can be even more helpful for understanding the nature of netwar.

---

<sup>6</sup>The success of Otpor (“Resistance”) in overthrowing the regime of Slobodan Milosevic in Serbia is an example of a combined insider-outsider strategy (Cohen, 2000).

<sup>7</sup>Stephen Borgatti and Peter Monge deserve special words of thanks for the informal review comments and significant criticisms they provided regarding this section.

Our main point is that netwar (and also counternetwar) is principally an organizational dynamic, even though it requires appropriate social and technological dynamics to work well. But our deeper point is that there is still much work to be done to clarify the meaning of “network” and come up with better, easier methods of analysis for policymakers and strategists. Both the social and organizational schools can contribute to this—but in different ways, because they have different tendencies.

### **Social Network Analysis<sup>8</sup>**

Social network analysis is an important academic specialty pursued by a relatively small number of anthropologists, sociologists, and organization theorists. It has grown in influence for several decades. Generally speaking, their view—see a book like *Networks and Organizations*, or *Social Structures: A Network Approach*, or *Social Network Analysis*, or the web site of the International Network for Social Network Analysis (INSNA)—holds that all social relationships, including all social organizations, can and should be analyzed as networks: that is, as sets of actors (nodes) and ties (links) whose relationships have a patterned structure.<sup>9</sup>

Social network analysis traces many of its modern roots back to efforts, decades ago, to develop sociograms and directed graphs to chart the ties among different actors in particular contexts—what gradually became known as a network. Later, some social network analysts, along with social psychologists and organizational sociologists who studied what were then called organization-sets, observed that networks often come in several basic shapes (or topologies): notably, *chain* or line networks, where the members are linked in a row and communications must flow through an adjacent actor before getting to the next; *hub*, star, or wheel networks, where members are tied to a central node and must go through it to communicate with each other; and *all-channel* or fully connected or full-matrix networks, where ev-

<sup>8</sup>Some of this subsection is verbatim from Ronfeldt (2000).

<sup>9</sup>The references are, respectively to books by Nohria and Eccles (1992); Wellman and Berkowitz (1997); and Wasserman and Faust (1994). The INSNA's web site is at [www.heinz.cmu.edu/project/INSNA/](http://www.heinz.cmu.edu/project/INSNA/).

everyone is connected to and can communicate directly with everyone else (from Evan, 1972).<sup>10</sup> Other shapes have also been identified (e.g., grids and lattices, as well as center/periphery networks and clique networks<sup>11</sup>); so have combinations and hybrids, as in sprawling networks with myriad nodes linked in various ways that are sometimes called “spider’s web” networks. Moreover, any particular network may itself be embedded within surrounding networks. Yet, few social network analysts say much about such typologies; their concern is usually to let the data sets speak for themselves.

Classic studies concern topics like friendship cliques among school children, interlocking memberships in corporate boards, job search and occupational mobility patterns that depend on personal connections, partnerships among business firms, and even the structure of the world economic and political system. When a social network analyst studies a primitive tribe, a hierarchical bureaucracy, or a market system, he or she searches for the formal and informal networks that undergird it and emphasizes their roles in making that social organization or system work the way it does (e.g., as in Granovetter, 1985).

In this view, power and influence depend less on one’s personal attributes (e.g., resources, attitudes, behaviors) than on one’s interpersonal relations—the location and character of one’s ties in and to the network. The “unit of analysis” is not so much the individual as it is the network in which the individual is embedded. Not unlike complexity theorists, social network analysts view a network as a systemic whole that is greater than and different from its parts. An essential aim is to show how the properties of the parts are defined by their networked interactions, and how a network itself functions to create opportunities or constraints for the individuals in it.

Many social network analysts stress the importance of location: as in whether an actor’s power and prestige stem from his “centrality” in a

---

<sup>10</sup>More complicated designs may be laid out, depending on how many nodes and variations in ties are taken into account. While we appreciate the simplicity of the three designs mentioned here, a more complex depiction of networks composed of three to five persons appears in Shaw (1976), which uses the term “comcon” instead of “all-channel.”

<sup>11</sup>For discussions of center/periphery and clique networks, see writings by Stephen Borgatti posted at [www.analytictech.com/borgatti/](http://www.analytictech.com/borgatti/).



network, or whether he has greater autonomy and potential power if he is located at a “structural hole”<sup>12</sup> (a kind of “nonredundant” location that can provide an opening or bridge to an actor in a nearby network). Other analysts stress the importance of the links between actors: whether the ties are strong (tightly coupled) or weak (loosely coupled), and what difference this may make for acquiring and acting on information about what is happening in and around the network.<sup>13</sup> Other questions may be asked about the overall “connectedness” of a network, and the degrees of “reciprocity” and “mutuality” that characterize flows and exchanges within it.

For social network analysts, then, what is keenly interesting about individuals is not their “human capital” (personal properties) but their “social capital” (interpersonal or relational properties). Social networks are often said to be built out of social capital. Many—the ones that tend to be favored in a society, such as business partnerships—thrive when mutual respect and trust are high. But the cohesion and operation of other social networks—such as illicit ones for access to drugs and prostitution—may not require much respect or trust.

Social network analyses tend to be intricately methodological, placing a premium on mathematical modeling and visualization techniques.<sup>14</sup> Although there are exceptions related to measures of efficiency and effectiveness, these analyses are generally not normative or prescriptive, in the sense of observing that one kind of network structure may be better than another for a particular activity, such as a business alliance or a social movement. Moreover, these analyses are not evolutionary, in the sense of observing that the network may be a distinct form of organization, one that is now coming into its

---

<sup>12</sup>Term from Burt (1992). See also his chapter in Nohria and Eccles (1992), and his writings posted at <http://gsbwww.uchicago.edu/fac/ronald.burt/research/>. The “structural hole” concept is quite prominent in the literature about social network analysis. Meanwhile, a somewhat similar, equally interesting concept is the “small world network” being developed separately by mathematicians. See footnote 19.

<sup>13</sup>Granovetter (1973) is the classic reference about strong versus weak ties; see Perrow (1979) about tightly versus loosely coupled systems.

<sup>14</sup>For a fascinating discussion of the history of visualization techniques, see Freeman (2000).

own. For many social network analysts, the network is the mother of all forms, and the world amounts to a network of networks.

### Organizational Network Analysis<sup>15</sup>

Organizational network analysts—or, since this phrase is not widely used, analysts who use network perspectives for studying organizational forms—utilize many of the methods and measures developed for social network analysis. But their approach is quite different—many of them view the network as a distinct form of organization, one that is gaining strength as a result of advances in communications. Also, many of them think that network forms of organization have advantages over other (e.g., hierarchical) forms, such as flexibility, adaptability, and speed of response. For social network analysts, almost any set of nodes (actors) that have ties amounts to a network. But for organizational analysts, that is not quite enough. They might ask, for example, whether the actors recognize that they are participating in a particular network, and whether they are committed to operating as a network.

This literature arises mainly in the fields of organizational and economic sociology, and in business schools. There are various accounts as to who, in recent decades, first called attention to the emergence of networked organizational designs. But most accounts credit an early business-oriented analysis (Burns and Stalker, 1961) that distinguished between *mechanistic* (hierarchical, bureaucratic) and *organic* (networked, though still stratified) management systems. The organic form was deemed more suited to dealing with rapidly changing conditions and unforeseen contingencies, because it has “a network structure of control, authority, and communication” along with a “lateral rather than vertical direction of communication” (p. 121).

Nonetheless, and despite other insightful efforts to call attention to network forms of organization (e.g., Perrow, 1979; Miles and Snow, 1986), decades passed before a school of thinking began to cohere.

---

<sup>15</sup>The discussion here, like the one in the prior subsection, is selective and pointed. For broader, thorough discussions of the various literatures on organizational forms and organizational network analysis, see Monge and Contractor (2001) and Monge and Fulk (1999).

One seminal paper in particular (Powell, 1990) looked beyond informal social networks to argue that formal organizational networks were gaining strength, especially in the business world, as a distinct design—distinct in particular from the “hierarchies and markets” that economic transaction theorists, some other organizational economists, and economic sociologists were accustomed to emphasizing.

[T]he familiar market-hierarchy continuum does not do justice to the notion of network forms of organization. . . . [S]uch an arrangement is neither a market transaction nor a hierarchical governance structure, but a separate, different mode of exchange, one with its own logic, a network (Powell, 1990, pp. 296, 301).

But this new thinking remained focused mostly on innovative approaches to economic organization and business competition.<sup>16</sup> Moreover, definitional issues remained (and still do) as to precisely what is and is not a network form of organization; often, a definition that may be appropriate in the business world might not apply well in other contexts, such as for analyzing networked social movements.

Since the early 1990s, the literature on networks has grown immensely. Yet, the distinctions between the social and organizational approaches to analysis remain sources of academic debate. An important effort to bridge the debate (Nohria and Eccles, 1992) focused on inquiring “whether ‘network’ referred to certain characteristics of any organization or whether it referred to a particular form of organization” (p. vii). The question was left unresolved—a lead-off author claimed the pro-form view was largely rhetorical, while the concluding authors implied the academic debate was less significant than the fact that business strategists were developing and applying the new form.<sup>17</sup> In contrast, a later effort by a set of scholars who believe the network is a distinct form of organization (DeSanctis and Fulk, 1999)

---

<sup>16</sup>For example, Miles and Snow (1992) discuss why network organizations in the business world may fail rather than succeed; and Kumar and Dissel (1996) discuss interorganizational business systems whose topologies correspond to chain, hub, or all-channel networks. Also see references in footnote 4.

<sup>17</sup>In that volume, Perrow (1992) sounds a new note when he concludes that the large, fully integrated firms so characteristic of American life may have eroding effects on civil society—and the growth of small firm networks may have revitalizing effects.

ends by noting how much work remains to be done to clarify this phenomenon and its relation to the advances in communications technology. A key task is to create better typologies, since the study of organizational forms still “tends to be dominated by such dichotic concepts as market versus hierarchy or bureaucratic versus post-bureaucratic” (p. 498).

Lately, these unsettled debates over how to think about networks have affected major writings about where societies as a whole may be headed. Consider, for example, this treatment in Francis Fukuyama's *The Great Disruption* (1999), which does not view networks as a distinctive form of organization that is newly on the rise:

If we understand a network not as a type of formal organization, but as *social capital*, we will have much better insight into what a network's economic function really is. By this view, a network is a moral relationship of trust: A network is a group of individual agents who share *informal* norms or values beyond those necessary for ordinary market transactions. The norms and values encompassed under this definition can extend from the simple norm of reciprocity shared between two friends to the complex value systems created by organized religions (Fukuyama, 1999, p. 199, italics in original).

This is different from the view espoused by Manuel Castells in *The Rise of the Network Society* (1996). He recognizes, in a manner not unlike Fukuyama, the importance that values and norms play in the performance of networks and other forms of organization. Yet, his deeper point is that networks are spreading and gaining strength as a distinct form of organization:

Our exploration of emergent social structures across domains of human activity and experience leads to an overarching conclusion: as a historical trend, dominant functions and processes in the information age are increasingly organized around networks. Networks constitute the new social morphology of our societies . . . . While the networking form of social organization has existed in other times and spaces, the new information technology paradigm provides the material basis for its pervasive expansion throughout the entire social structure (Castells, 1996, p. 469).

Fukuyama's view reflects mainly the social network approach to analysis, Castells's the organizational approach—and his view is more tied to the influence of the information revolution. Our own view is decidedly in the latter camp (Arquilla and Ronfeldt, 1996, 2000; Ronfeldt, 1992, 1996); but that is not the main point here. The point is that these debates are far from settled; they will persist for years. Meanwhile, where netwar is the object of concern—as in assessing the degree to which an adversary is or is not a netwar actor, and how well it is designed for particular strategies and tactics—the analyst should be steeped in the organizational as much as the social approach. Organizational design is the decisive factor (even when the actors are individuals).

Against this backdrop, good progress at network analysis is being made by anthropologists, sociologists, and political scientists who are studying the growing roles of organizational networks in social movements. Their definitions of “network” have not always improved on prior ones. For example, a pathbreaking study of transnational advocacy movements (Keck and Sikkink, 1998) defines networks rather vaguely as “forms of organization characterized by voluntary, reciprocal, and horizontal patterns of communication and exchange” (p. 8). But their full discussion considers all the organizational, doctrinal, technological, and social dynamics that an effective social movement—and netwar actor—requires.

As noted in Chapter One of this volume, one of the earliest studies to point in this direction was about SPIN (segmented, polycentric, ideologically integrated network) movements in the 1960s. This concept, though rarely noticed by scholars in either the social or the organizational school, remains relevant to understanding the theory and practice of netwar—which is why this volume includes Chapter Nine by Luther Gerlach, updating and summarizing his views about SPIN dynamics. While he has focused the SPIN concept on social movements in the United States, the concept also illuminates dynamics that are under development in various terrorist, criminal, ethnonationalist, and fundamentalist networks around the world.

Furthermore, complexity theorists in the hard and social sciences— theorists interested in discerning common principles to explain “the architecture of complexity” across all natural and human systems—

are delving into the structures and dynamics of biological, ecological, and social systems where networks are the organizing principle (e.g., see Strogatz, 2001). Of the many orderly patterns they have found, one seems particularly worth mentioning here. Many such systems feature a small number of highly connected nodes acting as hubs, along with a large number of less connected nodes—a pattern that proves resilient to systemic shocks, unless a key hub is disrupted or destroyed.<sup>18</sup> This apparently resembles a well-structured, multihub “spider’s web” network, or a set of interconnected center/periphery networks. Also, this is the kind of pattern—one or more actors as key hubs, around which are arrayed a large number of actors linked to the hubs but less so to each other, yet with frequent all-channel information-sharing across all actors—that was seen in the social networks in Seattle and in Mexico. It may also characterize some sprawling terrorist and criminal networks.

### **WHAT MAKES A NETWORK EFFECTIVE, BESIDES ORGANIZATION?<sup>19</sup>**

What holds a network together? What makes it function effectively? The answers involve much more than the organizational aspects emphasized above. While there is no standard methodology for analyzing network forms of organization, our familiarity with the theoretical literature and with the practices seen among netwar actors indicates that the design and performance of such networks depend on what happens across five levels of analysis (which are also levels of practice):<sup>20</sup>

---

<sup>18</sup>George Johnson, “First Cells, Then Species, Now the Web,” *The New York Times*, December 26, 2000, pp. M1, M2, provides an overview and relates how this pattern may reflect a mathematical “power law” that is of interest to complexity theorists.

<sup>19</sup>Some of the text in this section is from our earlier books (see Arquilla and Ronfeldt, 1996, 2000). What is analytically new here is the addition of the “narrative level” to the scope of analysis.

<sup>20</sup>This assumes that there are enough actors and resources to organize a network in the first place. Otherwise we would have to specify a recruitment and resource level as part of what makes a network strong and effective.

- Organizational level—its organizational design
- Narrative level—the story being told
- Doctrinal level—the collaborative strategies and methods
- Technological level—the information systems
- Social level—the personal ties that assure loyalty and trust.

The strength of a network, perhaps especially the all-channel design, depends on its functioning well across all five levels. The strongest networks will be those in which the organizational design is sustained by a winning story and a well-defined doctrine, and in which all this is layered atop advanced communications systems and rests on strong personal and social ties at the base. Each level, and the overall design, may benefit from redundancy and diversity. Each level's characteristics are likely to affect those of the other levels.

These are not idle academic issues. Getting a network form “right”—like getting a hierarchical or market form “right”—can be a delicate enterprise. For practitioners trying to organize a new network or adjust one that already exists, various options may merit consideration—and their assessment should assure that all the organizational, narrative, doctrinal, technological, and social levels are well-designed and integrated.

This applies to netwar and counternetwar actors across the spectrum. However, our discussion emphasizes evidence from social netwar actors, mainly activist NGOs, because they have been more open and expressive than have terrorist, criminal, and other violent, secretive actors. The discussion draws on some of the cases presented in earlier chapters, but also affords an opportunity to bring in other recent examples.

Each of these levels of analysis deserves more elaboration than we give here. Our goals are to get people to think in these terms and point the way, even though we cannot pretend to offer final methodological guidance.

## Organizational Level

To what extent is an actor, or set of actors, organized as a network? And what does that network look like? This is the top level—the starting point—for assessing the extent to which an actor, or set of actors, may be designed for netwar.

Nowadays, many writings about terrorists, criminals, and activists observe that one grouping or another is organized as a network. But the analyst should be able to specify more than simply that. Among other things, assessment at this level should include showing exactly what type of network design is being used, whether and how members may act autonomously, where leadership resides and/or is distributed, and whether and how hierarchical dynamics may be mixed in with the network dynamics.

As noted earlier, networks come in three major typologies: chain, hub, and all-channel. There are also complex combinations and hybrids involving myriad nodes and links—as in “spider webs,” as well as in center/periphery and clique networks. There are also designs that amount to hybrids of networks and hierarchies. In many cases, an important aspect may be the variety of “structural holes” and “bridges” that exist within and between networks—and whether “short cuts” exist that allow distant actors to connect with only a few hops across intermediates, as in a “small world network.”<sup>21</sup> Henry Mintzberg (1981) suggests that short cuts may be facilitated by the rise of “mutual adjustment” practices in cross-disciplinary teams. He notes this in the context of business organizations, where the “adjustment phenomenon” will break down “line and staff as well as a number of other distinctions” (p. 5).

Netwar analysts writing for policymakers and strategists should be able to identify and portray the details of a network’s structure—as well as they traditionally do when charting an adversary’s leadership structures, especially for analyzing terrorist and criminal groups.

---

<sup>21</sup>See Burt (1992, and his web site) on “structural holes” and “bridges,” and Watts (1999) and Strogatz (2001) on “small world networks.” Watts and Strogatz approach the study of complex networks as mathematicians.



In an archetypal netwar, the units are likely to resemble an array of dispersed, internettted nodes set to act as an all-channel network. Recent cases of social netwar by activist NGOs against state and corporate actors—e.g., the series of campaigns known as J18, N30, A16, etc.—show the activists forming into open, all-channel, and multihub designs whose strength depends on free-flowing discussion and information sharing. The chapters on Burma, Mexico, and the Battle of Seattle substantiate this.

In addition, the International Campaign to Ban Landmines (ICBL) is the prime case of a social netwar developed by NGO activists whose network eventually included some government officials, in a campaign that one prominent organizer, Jody Williams, called “a new model of diplomacy” for putting pressure on the United States and other recalcitrant governments:

It proves that civil society and governments do not have to see themselves as adversaries. It demonstrates that small and middle powers can work together with civil society and address humanitarian concerns with breathtaking speed. It shows that such a partnership is a new kind of “superpower” in the post-Cold War world. . . . For the first time, smaller and middle-sized powers had not yielded ground to intense pressure from a superpower to weaken the treaty to accommodate the policies of that one country (Jody Williams, 1997 *Nobel Lecture*, December 10, 1997, [www.wagingpeace.org/articles/nobel\\_lecture\\_97\\_williams.html](http://www.wagingpeace.org/articles/nobel_lecture_97_williams.html)).

This campaign had no central headquarters or bureaucracy. Instead, it had a netwar design—a pattern of constant, open communication and coordination among a network of national campaigns that worked independently but coordinated constantly with each other on behalf of their common goal (also see Williams and Goose, 1998).

Such flatness and openness may be impossible for terrorist, criminal, and other violent netwar actors who depend on stealth and secrecy; cellular networks and/or hierarchies may be imperative for them, along with hybrids of hierarchies and networks. Consider the Earth Liberation Front (ELF), a radical environmental group of unclear origins. The ELF may in fact have only a small core of true believers who commit its most violent acts, such as arson and vandalism at new

construction sites in naturally wild landscapes (e.g., Long Island, New York). But according to ELF publicist, Craig Rosebraugh, the ELF consists of a “series of cells across the country with no chain of command and no membership roll.” It is held together mainly by a shared ideology and philosophy. “There’s no central leadership where they can go and knock off the top guy and it will be defunct.”<sup>22</sup> In other words, the ELF is allegedly built around “autonomous cells” that are entirely underground. This is different from the “leaderless resistance” doctrine discussed later, which requires a mix of aboveground and underground groups. This is also different from those terrorist networks discussed in Chapter Two that are characterized by horizontal coordination among semiautonomous groups.

In netwar, leadership remains important, even though the protagonists may make every effort to have a leaderless design. One way to accomplish this is to have many leaders diffused throughout the network who try to act in coordination, without central control or a hierarchy. This can create coordination problems—a typical weakness of network designs—but, as often noted, it can also obviate counterleadership targeting. Perhaps a more significant, less noted point is that the kind of leader who may be most important for the development and conduct of a netwar is not the “great man” or the administrative leadership that people are accustomed to seeing, but rather the doctrinal leadership—the individual or set of individuals who, far from acting as commander, is in charge of shaping the flow of communications, the “story” expressing the netwar, and the doctrine guiding its strategy and tactics.

We often posit that it may take networks to fight networks. Yet, government interagency designs for waging counternetwar against terrorists, criminals, and other violent, law-breaking adversaries will have to be built around hybrids of hierarchies and networks. Governments cannot, and should not, attempt to do away with all hierar-

---

<sup>22</sup>From Dan Barry and Al Baker, “Getting the Message from ‘Eco-Terrorists’: Mystery Group Takes Its Campaign East,” *The New York Times*, January 8, 2001, A15. The ELF sometimes operates in alliance with the Animal Liberation Front. See the web site at [www.earthliberationfront.com](http://www.earthliberationfront.com).

chy.<sup>23</sup> Earlier chapters, especially the ones on dealing with terrorists, criminals, and gangs, expanded on this point.

## Narrative Level

Why have the members assumed a network form? Why do they remain in that form? Networks, like other forms of organization, are held together by the narratives, or stories, that people tell.<sup>24</sup> The kind of successful narratives that we have in mind are not simply rhetoric—not simply a “line” with “spin” that is “scripted” for manipulative ends. Instead, these narratives provide a grounded expression of people’s experiences, interests, and values.<sup>25</sup> First of all, stories express a sense of identity and belonging—who “we” are, why we have come together, and what makes us different from “them.” Second, stories communicate a sense of cause, purpose, and mission. They express aims and methods as well as cultural dispositions—what “we” believe in, and what we mean to do, and how.

The right story can thus help keep people connected in a network whose looseness makes it difficult to prevent defection. The right story line can also help create bridges across different networks. The

---

<sup>23</sup>We have previously discussed the need for attention to hybrids of hierarchies and networks, most recently with regard to military swarming (Arquilla and Ronfeldt, 2000). Yet, the idea that such hybrids are a normal feature of social life has figured in a substream of academic writings for decades. In an exemplary volume from the 1970s (La Porte, 1975), the authors maintain that few social activities have structures that look like a “tree” (hierarchy) or a “full matrix” (an all-channel network). Most have “semilattice” structures—they resemble a set of oddly interconnected hierarchies and networks.

<sup>24</sup>Because we want to encourage a new turn of mind, we discuss this as the narrative level, in keeping with our sense that “whose story wins” is a vital aspect of netwars of all types. We could have also presented this level of analysis in a more traditional light, as a cultural, ideological, and/or political level, but the concepts of “narratives” and “stories” seem equally useful and more dynamic for capturing how people actually communicate with each other.

<sup>25</sup>This has been a strong theme of American radical activist organizers, from early pre-netwar ones like Saul Alinsky to contemporary strategists like Gene Sharp.

right story can also generate a perception that a movement has a winning momentum, that time is on its side.<sup>26</sup>

Doctrinal and other leaders may play crucial roles in designing winning stories and building organizational cultures around them. This has long been recognized for executives in corporate systems.<sup>27</sup> It is also true for netwar actors.

All the netwar actors examined in this volume engage in narrative assurance, and use old and new media to do so. All are very sensitive about the stories they use to hold a network together and attract external audiences. For terrorists, the stories tend to herald heroic deeds, for criminals their adventures in greed, and for social activists their campaigns to meet human needs. If it sounds odd to cast criminals this way, note that Colombian (not to mention Mexican and other) drug traffickers have no problem viewing and presenting themselves in a positive light as archnationalists who do good for their communities, for example through financial donations to churches, hospitals, and schools, as well as through legitimate investments in sagging local economies.

On this point, Manuel Castells (1998, pp. 196–201) discusses cartel behavior in Colombia to underscore his thesis (p. 197) about “the importance of cultural identity in the constitution, functioning, and strategies of criminal networks.”

The attachment of drug traffickers to their country, and to their regions of origin, goes beyond strategic calculation. They were/are deeply rooted in their cultures, traditions, and regional societies. Not only have they shared their wealth with their cities, and invested a

---

<sup>26</sup>This, of course, is true for earlier modes of conflict too. Modern guerrilla wars placed very strong emphasis on winning by convincing an opponent that an implacable insurgent movement can never be decisively defeated. In counterinsurgency, similar efforts are made to win the “hearts and minds” of indigenous peoples.

<sup>27</sup>According to a classic of organization theory (Schein, 1985, p. 2), “there is a possibility . . . that the only thing of real importance that leaders do is to create and manage culture.” According to Bran Ferren, former Walt Disney Imagineering executive, “The core component of leadership is storytelling, how to articulate a vision and communicate it to people around you to help accomplish the mission” (see Tony Perry, “Navy Takes a Scene Out of Hollywood,” *Los Angeles Times*, November 27, 2000, pp. C1, C5, on Ferren’s design of a new command center for a Navy command ship).

significant amount (but not most) of their fortune in their country, but they have also revived local cultures, rebuilt rural life, strongly affirmed their religious feelings, and their beliefs in local saints and miracles, supported musical folklore (and were rewarded with laudatory songs from Colombian bards), made Colombian football teams (traditionally poor) the pride of the nation, and revitalized the dormant economies and social scenes of Medellin and Cali—until bombs and machine guns disturbed their joy (p. 199).

In the abstract, his points might apply as well to some leading terrorist groups in the Middle East.

Writings about social activism are especially keen about the narrative level. Keck and Sikkink (1998, citing Deborah Stone) observe that it is crucial for social campaigns to follow the lines of a “strategic portrayal” based on a “causal story.” Rutherford (1999) relates the growth of the ICBL to the story it choose to tell: “By controlling the agenda—what was to be discussed and how—the ICBL established the context of the landmine debate as humanitarian rather than military.” Also, Otpor (“Resistance”), the netwar-like underground movement to overthrow Milosevic and democratize Serbia, adopted a doctrine of nonviolence, not simply because that was the ethical thing to do, but because it would help provoke the regime into resorting to force in ways that would undermine its authority and give Otpor the high ground regarding whose story should win (Cohen, 2000).

Military campaigns also depend on whose story wins. For example, the highly networked Chechens won their military campaign against Russia during the 1994–1996 war—and they also won the battle of the story, portraying themselves as plucky freedom fighters ridding their land of the last vestiges of a tottering, evil old empire. But in the second war, beginning in 1999, the Russians not only improved their own ability to fight in small, dispersed, networked units, but also mobilized Russian society, including many organizations that opposed the first war in Chechnya, by portraying this second round as a war against terrorism. This story, advanced in the wake of urban bombings in Russia in 1999, even played well in the industrialized West, which has given the Russians a free hand in Chechnya this time, with no threats to withhold new loans because of what might be going on in the transcaucasus region.

In the current Intifadah, both the Palestinians and the Israelis have waged an ever-shifting “battle of the story.” The Palestinians have depicted the Israelis as having abrogated the Oslo Accord, while the Israelis have depicted Arafat and his advisers as unwilling to make any—even reasonable—concessions. Moreover, the Palestinians have portrayed the Israelis as using excessive force—although this thrust is vitiated by the Palestinians own violent acts. Meanwhile in cyberspace, both sides have reached out successfully to their ethnic diasporas, for moral as well as financial support. Both have also successfully encouraged distributed-denial-of-service (DDOS) attacks on each other’s information systems—the Israelis going so far as to provide a web site for encouraging average Israeli citizens to join the cause by downloading and using various computer attack tools. The Palestinians have used a narrative-level twist on this—they have invoked a “cyber jihad” against Israel, which has resulted in much participation in the cyberspace aspects of this conflict by Muslims from Morocco to Pakistan. Hizbollah in particular has articulated a strategy that includes both computerized swarming attacks on Israeli information infrastructures and selective attacks on commercial firms doing business with Israel.<sup>28</sup>

Disinformation, misrepresentation, and outright lying are eternal downsides that should not be overlooked at the narrative level. Some actors may be unscrupulously cunning about the story lines they unfold in the media.<sup>29</sup> Nonetheless, many of the major trends of the information age—e.g., the continued growth of global media of all types, the proliferation of sensors and surveillance devices, the strengthening of global civil society—imply that the world will become ever more transparent. This may well be a mixed blessing, but it should be to the advantage of democratic state and nonstate actors who thrive on openness (Florini, 1998; Brin, 1998).

<sup>28</sup>Lee Hockstader, “Pings and E-Arrows Fly in Mideast Cyber-War,” *Washington Post Foreign Service*, October 27, 2000. Carmen Gentile, “Israeli Hackers Vow to Defend,” *Wired News*, November 15, 2000.

<sup>29</sup>Gowing (1998) provides a distressing account of how well-meaning but naïve and presumptuous humanitarian NGOs were outmaneuvered by Rwandan officials and their allies in the battle for the control and manipulation of information in the Great Lakes region of Africa in the mid 1990s. Rothkopf (1999), among others, warns about the advent of “the disinformation age,” although his examples are not from netwars.

As this occurs, a premium will be placed on using public diplomacy to advance one's messages. Jamie Metz (1999, pp. 178, 191) explains that

the struggle to affect important developments across the globe is increasingly an information struggle. Without winning the struggle to define the interpretation of state actions, the physical acts themselves become less effective. . . . [T]he culture of foreign policy must change from one that along with protecting secrets and conducting secret negotiations recognizes that openness—achieved through the development of broad information networks and multiple temporary mini-alliances with both state and nonstate actors—will be the key to foreign policy success.

This may give presumably weaker actors, like NGOs intent on social netwar, a soft-power edge in dealing with presumably stronger actors, like states. As Martin Libicki (1999–2000, p. 41) argues,

The globalization of perception—the ability of everyone to know what is happening in minute detail around the world and the increasing tendency to care about it—is another way that the small can fend off the large.

Many approaches are being developed for analyzing the narrative level—for example, by scholars who study soft power, political discourse, narrative paradigms, story modeling, agenda setting, metaphors, frames, messages, and/or perspective-making. Some approaches reflect established social-science efforts to understand psychology, propaganda, ideology, and the media, and, in the field of political science, to develop a norm-oriented “constructivist” paradigm as an alternative to the dominant “neorealist” paradigm.<sup>30</sup> Other approaches reflect the rise of “postmodernism” in academia (as in the writings of Pierre Bourdieu, Jacques Derrida, Michel Foucault,

---

<sup>30</sup>Standard sources on neorealism include a range of writings by Kenneth Waltz and John Mearshimer in particular. The literature on constructivism is much more recent and less settled but revolves mainly around writings by Emanuel Adler, Peter Katzenstein, Terrence Hopf, and Alexander Wendt, among others. An interesting effort to split the difference, by focusing on how people argue their stories, is Risse (2000). Our own interest in the narrative level stems in part from our work on the concept of “noopolitik” (Arquilla and Ronfeldt, 1999, and Ronfeldt and Arquilla, 2000).

and Gilles Deleuze and Felix Guattari). All of them show the importance of this level of analysis and practice.

## Doctrinal Level

What doctrines exist for making best use of the network form of organization? This level of analysis is very important for explaining what enables the members to operate strategically and tactically, without necessarily having to resort to a central command or leader. The performance of the multihub and all-channel designs in particular may depend on the existence of shared principles and practices that span all nodes and to which the members subscribe in a deep way. Such a set of guiding principles and practices—a doctrine—can enable them to be “all of one mind” even though they are dispersed and devoted to different tasks. It can provide a central ideational, strategic, and operational coherence that allows for tactical decentralization. Overall, this is a looser approach to decisionmaking and operations than traditionally found in right- or left-wing movements—compare this approach, for example, to Mao Zedong’s maxim that “command must be centralized for strategic purposes and decentralized for tactical purposes.”

So far, two doctrinal practices seem particularly apt for netwar actors. One is to organize and present a network in a way that is as “leaderless” as possible, by having no single leader who stands out, by having (or appearing to have) multiple leaders, and by using consultative and consensus-building mechanisms for decisionmaking.<sup>31</sup> This principle is quite evident in several cases in this book. The second is to use swarming strategies and tactics by having myriad small units that are normally kept dispersed turn to converge on a target from all directions, conduct an attack, and then redisperse to prepare for the next operation. This second principle—swarming—has not been explicitly espoused or adopted by the actors we have looked at, but it is implicitly there, awaiting refinement in many of them—from Middle Eastern terrorists seeking to enter the United States from different di-

---

<sup>31</sup>Commonly recognized downsides are the possibilities that no decision is made, that unaccountable ones are made, or that a network will lack a “center of gravity.”



rections in order to converge on a bombing target, to NGO activists who swarmed into Mexico in 1994 and Seattle in 1999.

An example of the first principle is the doctrine of “leaderless resistance” elaborated by right-wing extremist Louis Beam. This doctrine downplays hierarchy in favor of organizing networks of “phantom cells.” It reveals a belief that the more a movement conforms to a networked organizational style, the more robust it will be defensively, and the more flexible offensively:

Utilizing the Leaderless Resistance concept, all individuals and groups operate independently of each other, and never report to a central headquarters or single leader for direction or instruction. . . . [P]articipants in a program of Leaderless Resistance through Phantom Cell or individual action must know exactly what they are doing, and exactly how to do it. . . . Organs of information distribution such as newspapers, leaflets, computers, etc., which are widely available to all, keep each person informed of events, allowing for a planned response that will take many variations. No one need issue an order to anyone (Beam, 1992).

The underground element of Beam’s doctrine originally called for four types of secretive, decentralized cells: command, combat, support, and communiqué cells. Each should consist of about eight “minutemen” and have its own leader. But late in the 1990s, practice diverged from this doctrine, allowing “lone wolves” to instigate violent acts, like bombings, seemingly on their own initiative.

The leaderless resistance doctrine has permeated far right circles in the United States (see Burghardt, 1995a, 1995b; Stern, 1996).<sup>32</sup> In addition, it has reached hate groups in Germany, some of which are stockpiling weapons and explosives and posting death lists on web sites.

“What we are seeing is a very worrying trend in the organization of far right groups with a view to committing terrorism,” says Graeme

---

<sup>32</sup>According to Paul de Armond, many far rightists may now regard leaderless resistance as a backward step, since it means that they should not, indeed cannot, organize a mass party and be very public about their leaders and aims. See Barkun (1997) for further discussion of leaderless resistance.

Atkinson, European editor of the anti-fascist magazine *Searchlight*. "They are talking about creating a 'leaderless resistance' of terrorist cells—and of ensuring the creation of liberated zones, with foreigners driven out from rural areas and smaller towns" (Martin A. Lee, "Neo-Nazism: It's Not Just in Germany's Beer Halls Anymore," *Los Angeles Times*, December 31, 2000, p. M2).

By itself, a tenet like leaderless resistance is only a partial step toward having a doctrine for netwar. What operational behavior may in fact be most effective for small, dispersed, mobile forces that are joined in networks? The short answer is swarming (for elaboration, see Arquilla and Ronfeldt, 1997, 2000). If the optimal organizational form for netwar is the dispersed network, the corresponding doctrine must surely consist of swarming. Swarming may well become the key mode of conflict in the information age. But swarming doctrines and strategies have barely begun to emerge for the conduct of terrorist, criminal, and social conflicts.

In this volume, the Zapatista and Seattle cases show swarming in action. Today, one of the most sophisticated doctrines for social netwar comes from the Direct Action Network (DAN), which arose from a coalition of activists dedicated to using nonviolent direct action and civil disobedience to halt the WTO meeting in Seattle. Its approach to netwar epitomizes swarming ideas. Participants are asked to organize, at their own choice, into small (5–20 people) "affinity groups"—"self-sufficient, small, autonomous teams of people who share certain principles, goals, interests, plans or other similarities that enable them to work together well."<sup>33</sup> Each group decides for itself what actions its members will undertake, ranging from street theater to risking arrest.<sup>34</sup> Where groups operate in proximity to each other, they are further organized into "clusters"—but there may also be "flying groups" that move about according to where needed. Different people in each group take up different functions (e.g., police liaison), but every effort is made to make the point that no group has a single lead-

---

<sup>33</sup>See DAN's web site, [www.directactionnetwork.org/](http://www.directactionnetwork.org/). It is the source of the observations and quotations in the paragraph.

<sup>34</sup>One role in an affinity group might be police liaison, but it carries the risk that this person would be perceived as a group leader, when in fact the group does not have a leader per se, making all decisions through consensus.

er. All this is coordinated at spokescouncil meetings where each group sends a representative and decisions are reached through democratic consultation and consensus (in yet another approach to leaderlessness).

This approach generated unusual flexibility, mobility, and resource sharing in the Battle of Seattle. It is discussed at length in Chapter Seven, but here is another eyewitness account:

In practice, this form of organization meant that groups could move and react with great flexibility during the blockade. If a call went out for more people at a certain location, an affinity group could assess the numbers holding the line where they were and choose whether or not to move. When faced with tear gas, pepper spray, rubber bullets and horses, groups and individuals could assess their own ability to withstand the brutality. As a result, blockade lines held in the face of incredible police violence. When one group of people was finally swept away by gas and clubs, another would move in to take their place. Yet there was also room for those of us in the middle-aged, bad lungs/bad backs affinity group to hold lines in areas that were relatively peaceful, to interact and dialogue with the delegates we turned back, and to support the labor march that brought tens of thousands through the area at midday. No centralized leader could have coordinated the scene in the midst of the chaos, and none was needed—the organic, autonomous organization we had proved far more powerful and effective. No authoritarian figure could have compelled people to hold a blockade line while being tear gassed—but empowered people free to make their own decisions did choose to do that (Starhawk, *How We Really Shut Down the WTO*, December 1999, [www.reclaiming.org/starhawk/wto.html](http://www.reclaiming.org/starhawk/wto.html)).

This is very much a netwar doctrine. It is not quite an explicit swarming doctrine—but almost.

An unusually loose netwar design—one that is eminently leaderless yet manages to organize a large crowd for a rather chaotic, linear kind of swarming—is found in the pro-bicycle, anti-car protest movement known as Critical Mass (CM) in the San Francisco Bay area. Since its inception in 1992, CM's bicycle activists (sometimes numbering 2,000) have converged on the last Friday of every month from around the Bay area to disrupt traffic at peak hours along a chosen route.

They slow and block traffic, while handing out pamphlets about pollution and other detriments of the automobile culture. CM riders are proud of their lack of formal organization and leadership and constitute what they call a “xerocracy,” which amounts to governance by distributing copies of an idea online or on the scene, say for a ride route, and letting a vote by the assembled decide. A key doctrinal tenet is “organized coincidence,” by which “CM rides simply ‘materialize’ every month even though there are no leaders or organizational sponsorships.” This way, “No one need take responsibility but everyone can take credit.”

The aim is to ride en masse. The preference may be for “keeping Mass” (riding in a single, large, spread-out mass), but for safety or other reasons a ride may splinter into “minimasses” (multiple, dense small groups). Group decisionmaking about when and where to alter the route of a ride may occur on the fly, as a function of “dynamic street smarts” among the bicyclists up front. A “buddy system” is used to watch out for each other within a mass. Whistle signals are used for some command and control (e.g., stop, go, turn). “Cell phone contact” is used for communications between minimasses, which is particularly helpful if riders want to regroup splinters into a single mass. Tactics during a ride may include “corking” an intersection and “swarming” around a lone car. For much of the 1990s, there were tendencies for confrontation—if not by the riders then by police who came to “escort” and “herd” them. But by 1999, CM became “a ride dominated by creative self-governance and celebratory experimentation—with little or no ill will, and an eye out for avoiding confrontation.”<sup>35</sup>

In netwars, swarming often appears not only in real-life actions but also through measures in cyberspace. Aspirations for a leaderless swarming doctrine, beginning with a rationale and a capability for

---

<sup>35</sup>Sources are Dylan Bennett and Gretchen Giles, “Spokes Persons: Bicyclists See Transportation As Critical,” *Sonoma County Independent*, April 3–9, 1997, [www.metroactive.com/papers/sonoma/04.03.97/bikes-9714.html](http://www.metroactive.com/papers/sonoma/04.03.97/bikes-9714.html); *Critical Mass*, undated brochure, <http://danenet.wicp.org/bcp/cm.html>; Joel Pomerantz, *A San Francisco Critical Mass Glossary: 7 Years of Building a Culture & Learning Lessons, As Reflected in Our Terminology*, September 1999, <http://bok.net/~jig/CM/glossary.html>; and Joel Pomerantz, *A Few Comments on Critical Mass: A Brief Introduction to the Critical Mass Glossary*, October 1999, <http://bok.net/~jig/CM/glossaryintro.html>.

“electronic civil disobedience,” show up among hacktivists who advocate the usage of online tools to flood (i.e., overwhelm) a target’s computer systems, email inboxes, and web sites, thereby disrupting and even defacing them (see Wray, 1998). Virtually anybody can log into one of these tools and, with a few commands, mount an automated DDOS attack. For example, a device called FloodNet, developed by a collectivity named the Electronic Disturbance Theater (EDT), has been used since the late 1990s against government and corporate sites in Mexico, the Middle East, Europe, and the United States (e.g., against Etoys). Hacktivists associated with the EDT would like to create a new device named SWARM (after our writings), in order to move “digital Zapatismo” beyond the initial emphasis on FloodNet and create new kinds of “electronic pulse systems” for militant activism.<sup>36</sup>

A newer device, called Tribal FloodNet, evidently programmed by a German hacker named Mixer, is technically more powerful. It can enable a lone anonymous individual to mount a far more massive DDOS attack than is the case with FloodNet, which requires publicly announced mass participation (a virtual sit-in) to function well. Tribal FloodNet gained notoriety for its usage in shutting down Yahoo! and other U.S. sites early in 2000. But since then, the contrast between the two systems has led to an ideological controversy. Hacktivist proponents of FloodNet—not only in the EDT, but also in the Electrohippies and, to a lesser extent, the Cult of the Dead Cow—prefer to assert “the presence of a global group of people gathering to bear witness to a wrong.” They criticize the Tribal version for being undemocratic and secretive.<sup>37</sup>

<sup>36</sup>Interested readers should visit [www.nyu.edu/projects/wray/](http://www.nyu.edu/projects/wray/) and related web sites.

<sup>37</sup>From Stefan Krempel, “Computerized Resistance After the Big Flood: Email Interview with Ricardo Dominguez,” *Telepolis* (European online magazine), February 16, 2000, [www.heise.de/tp/english/inhalt/te/5801/1.html](http://www.heise.de/tp/english/inhalt/te/5801/1.html); and Carrie Kirby, “Hacking with a Conscience Is a New Trend,” *San Francisco Chronicle*, November 20, 2000, posted at [www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/11/20/BU121645.DTL](http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/11/20/BU121645.DTL). Also see the web sites of the EDT, the Electrohippies, and the Cult of the Dead Cow.

## Technological Infrastructure

What is the pattern of, and capacity for, information and communications flows within an organizational network? What technologies support them? How well do they suit the organizational design, as well as the narrative and doctrinal levels? The new information and communications technologies are crucial for enabling network forms of organization and doctrine. An ample, blossoming literature speaks to this (e.g., DeSanctis and Fulk, 1999). Indeed, the higher the bandwidth and the more dispersed the means of transmission, reception, storage, and retrieval, the better the prospects for success with network-style organization. The multihub and all-channel designs in particular depend on having a capacity—an infrastructure—for the dense communication of functional information. Current advances in peer-to-peer computing (as seen with Napster, Publius, and FreeNet) may give netwar actors an even greater technological edge in the future.<sup>38</sup>

Yet, as noted in Chapter One, netwar can be waged without necessarily having access to the Internet and other advanced technologies. This level may mix old and new, low- and high-tech capabilities. Human couriers and face-to-face meetings may still remain essential, especially for secretive actors like terrorists and criminals.

Many of the chapters in this volume speak to these points. Additional evidence comes from other interesting cases of netwar. Consider the development of the ICBL. Its protagonists got the movement off the ground in the early 1990s by relying mainly on telephones and faxes. They did not turn to the Internet until the mid 1990s, using it first for internal communication and later to send information to outside actors and to the media. Thus, it is “romanticized gobbledygook” that the Internet was essential for the ICBL’s early efforts—email and web technologies were not widely used until late in the development of the campaign, and even then usage remained quite limited, rarely including government officials. Nonetheless, the late turn to the new

---

<sup>38</sup>We thank Bob Anderson of RAND for pointing out the importance of peer-to-peer computing. He observes that peer-to-peer computing can enable its users to prevent censorship of documents, provide anonymity for users, remove any single point of failure or control, efficiently store and distribute documents, and provide plausible deniability for node operators.

technologies did improve communication and coordination and helped the ICBL create, and present to the world, a sense that it was a close-knit community on the move, with an important story for the world to hear. A leading academic analyst of the ICBL's use of technology, Ken Rutherford (1999)<sup>39</sup> concludes,

One of the most significant aspects of the ICBL case is that it shows how NGO coalitions can use communications technologies in order to increase their opportunities for success in changing state behavior. It highlights the importance of how NGOs might be able to address security and social issues that states have thus far proven unable to manage. . . . [T]he role of communications technologies in future international NGO coalitions will be more important than they were in the landmine case.

That is in the case of a well-organized movement. But the new technologies can also have a catalyzing effect for the rapid, unexpected emergence of a spontaneous protest movement. Evidence for this—and for the further spread of the netwar phenomenon—appeared during a wild week in Britain in September 2000, when about 2,000 picketing protesters, alarmed by soaring gasoline prices, quickly organized into dispersed bands that blocked fuel deliveries to local gas stations. The protestors were brought together by cell phones, CB radios, in-cab fax machines, and email via laptop computers. They had no particular leader, and their coordinating center constantly shifted its location. Will Hutton, director general of Britain's Industrial Society (a probusiness group), called it “a very 21st-century crisis made possible by information technology”:

Old organizational forms have been succeeded by a new conception, the network. . . . Using mobile phones, people with no experience of protest were able to coalesce around common aims while never actually meeting.<sup>40</sup>

<sup>39</sup>Rutherford (1999), with original text corrected via email correspondence. Also see Williams and Goose (1998, esp. pp. 22–25).

<sup>40</sup>Alexander MacLeod, “Call to Picket Finds New Ring in Britain's Fuel Crisis,” *The Christian Science Monitor*, September 19, 2000. MacLeod notes that recent commercial practices increased Britain's vulnerability to this social netwar: Many tanker drivers were freelancers, with no contractual obligations to the oil companies; and many gas stations operated under a “just-in-time” delivery system, keeping few reserves in place.

An earlier example of the use of advanced communications in support of a protest movement can be found in the Polish Solidarity movement of the 1980s. In the wake of the imposition of martial law, mass arrests and some brutality, Solidarity had difficulties keeping its members mobilized and informed. The United States, which was actively trying to undermine communist rule, went to great lengths to provide the movement with sophisticated communications equipment that could not easily be monitored or located. The new gear re-empowered the movement, giving it the ability to once again mount strikes and demonstrations that repeatedly took the government (and the KGB) by surprise.<sup>41</sup>

### **Social Underpinnings**

The full functioning of a network also depends on how well, and in what ways, the members are personally known and connected to each other. This is the classic level of social network analysis, where strong personal ties, often ones that rest on friendship and bonding experiences, ensure high degrees of trust and loyalty. To function well, networks may require higher degrees of interpersonal trust than do other approaches to organization, like hierarchies. This traditional level of theory and practice remains important in the information age.

In this book, the chapters on terrorist, criminal, and gang organizations referred to the importance of kinship, be that of blood or brotherhood. Meanwhile, news about Osama bin Laden and his network, al-Qaeda (The Base), continue to reveal his, and its, dependence on personal relationships he formed over the years with “Afghan Arabs” from Egypt and elsewhere who were committed to anti-U.S. terrorism and Islamic fundamentalism. In what is tantamount to a classic pat-

---

<sup>41</sup>Schweizer (1994) details the CIA's sending of advanced communications devices to Solidarity, and notes (p. 146) that “the administration also wanted the underground fully equipped with fax machines, computers, advanced printing equipment, and more.” Woodward (1987, p. 66) observes that these secure lines of communication were also used to maintain contact with the CIA, which often gave Solidarity early warning of the military regime's planned “sweeps” for activists and leaders.



tern of clan-like behavior, his son married the daughter of his long-time aide and likely successor, Abu Hoffs al-Masri, in January 2001.<sup>42</sup>

The chapters on activist netwars also noted that personal friendships and bonding experiences often lie behind the successful formation and functioning of solidarity and affinity groups. And once again, the case of the ICBL speaks to the significance of this level, when organizer Jody Williams treats trust as the social bedrock of the campaign:

It's making sure, even though everybody was independent to do it their own way, they cared enough to keep us all informed so that we all had the power of the smoke-and-mirrors illusion of this huge machinery. . . . And it was, again, the follow up, the constant communication, the building of trust. Trust, trust, trust. The most important element in political work. Once you blow trust, you've blown it all. It's hard to rebuild.<sup>43</sup>

The tendency in some circles to view networks as amounting to configurations of social capital and trust is helpful for analyzing this level. But there are other important concepts as well, notably about people forming “communities of practice” (Brown and Duguid, 2000), “communities of knowing,” and “epistemic communities” (Haas, 1992). In a sense, all these concepts reflect the ancient, vital necessity of belonging to a family, clan, or tribe and associating one's identity with it.

Meanwhile, the traditions of social network analysis and economic transaction analysis warn against the risks of having participants who are “free riders” or lack a personal commitment to teamwork. Indeed, compared to tribal/clan and hierarchical forms of organization, networks have more difficulty instilling, and enforcing, a sense of personal identity with and loyalty to the network. This is one of the key weaknesses of the network form—one that may affect counternetwar

---

<sup>42</sup>See the three-part series of articles in *The New York Times* on “Holy Warriors,” beginning with Stephen Engelberg, “One Man and a Global Web of Influence,” *The New York Times*, January 14, 2001, pp. A1, A12–A13.

<sup>43</sup>From the discussion following the speech by Jody Williams, *International Organization in the International Campaign to Ban Landmines*, at a gathering of recipients of the Nobel Peace Prize, University of Virginia, November 6, 1998, [www.virginia.edu/nobel/transcript/jwilliams.html](http://www.virginia.edu/nobel/transcript/jwilliams.html).

designs as well. It extends partly from the fact that networks are often thought to lack a “center of gravity” as an organization.

## THE PRACTICE OF NETWAR (AND COUNTERNETWAR)

Netwar actors that are strong at all five levels are, and will be, very strong indeed. Netwar works—and it is working for all types: good guys and bad guys, civil and uncivil actors. So far, all have done quite well, generally, in their various confrontations with nation states. A significant question, then, is whether one or the other type could predominate in the future? Will NGOs proselytizing for human rights and high ethical standards reshape the world and its statecraft? Or will violent terrorists, criminals, and ethnonationalists have greater impact—in a dark way? Or will all types move ahead in tandem?

### Growing Recognition of Netwar’s Dark Face

Practice has been outrunning theory in one area after another where netwar is taking hold. Most commentaries and case studies about organizational networks (and networked organizations) have concerned competitive developments in the business world. However, the year 2000 brought an advance in U.S. government thinking about networking trends among our adversaries, and in the consideration of new options for dealing with them. Government- and military-related research institutes paid the most attention (e.g., see Copeland, 2000),<sup>44</sup> but high-level offices and officials were not lagging far behind.

The first landmark was the annual report, *Patterns of Global Terrorism: 1999*, released by the U.S. State Department’s Office of the Coordinator for Counterterrorism in April 2000. It provided the strongest statement yet about networking trends:

U.S. counterterrorist policies are tailored to combat what we believe to be the shifting trends in terrorism. One trend is the shift from well-organized, localized groups supported by state sponsors to loosely organized, international networks of terrorists. Such a net-

---

<sup>44</sup>In Copeland (2000), see especially the statements by James Rosenau and Steven Metz.

work supported the failed attempt to smuggle explosives material and detonating devices into Seattle in December. With the decrease of state funding, these loosely networked individuals and groups have turned increasingly to other sources of funding, including private sponsorship, narcotrafficking, crime, and illegal trade.<sup>45</sup>

By December 2000, observation of this trend—and of the links growing between crime and terrorism—became even more pronounced in the report of a U.S. interagency group on global crime. While noting that most criminal organizations remain hierarchical—they still have leaders and subordinates—the *International Crime Threat Assessment* found that:

International criminal networks—including traditional organized crime groups and drug-trafficking organizations—have taken advantage of the dramatic changes in technology, world politics, and the global economy to become more sophisticated and flexible in their operations. They have extensive worldwide networks and infrastructure to support their criminal operations . . . Much more than in the past, criminal organizations are networking and cooperating with one another, enabling them to merge expertise and to broaden the scope of their activities. Rather than treat each other as rivals, many criminal organizations are sharing information, services, resources, and market access according to the principle of comparative advantage.<sup>46</sup>

Also in December, a forecasting report with a 15-year outlook—*Global Trends 2015*—was produced by the National Intelligence Council, based largely on conferences sponsored by the Central Intelligence Agency for consulting nongovernment experts.<sup>47</sup> The report often us-

---

<sup>45</sup>From the "Introduction" to *Patterns of Global Terrorism: 1999*, Department of State Publication 10687, Office of the Secretary of State, Office of the Coordinator for Counterterrorism, released April 2000, [www.state.gov/www/global/terrorism/1999report/1999index.html](http://www.state.gov/www/global/terrorism/1999report/1999index.html).

<sup>46</sup>From U.S. Government Interagency Working Group, *International Crime Threat Assessment*, December 2000, Chapter 1, [www.whitehouse.gov/WH/EOP/NSC/html/documents/pub45270/pub45270chap1.html#4](http://www.whitehouse.gov/WH/EOP/NSC/html/documents/pub45270/pub45270chap1.html#4).

<sup>47</sup>National Intelligence Council, *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts*, NIC 2000-02, Central Intelligence Agency, December 2000, [www.cia.gov/cia/publications/globaltrends2015/index.html](http://www.cia.gov/cia/publications/globaltrends2015/index.html).

es the word “network” and observes that the world and many of its actors, activities, and infrastructures are ever more networked. Nonetheless, network dynamics appear more in a background than a foreground role—the report does not do much to illuminate network dynamics. Moreover, where this future outlook highlights the growing power and presence of networked nonstate actors of all varieties, it mostly plays up the perils of terrorists, criminals, and other possible adversaries, along with the challenges that activist NGOs may pose for states. The report has little to say about the promising opportunities for a world in which civil-society actors continue to gain strength through networking and where states may learn to communicate, coordinate, and act conjointly with them to address legitimate matters of mutual concern, from democracy to security.

### **Nationalism, Globalism, and the Two Faces of Netwar**

Which face of netwar predominates will depend on the kind of world that takes shape. The key story lines of the 20th century have come to an end. Imperialism, for example, has been virtually extirpated. Over half the world’s landmass was under colonial control in 1900,<sup>48</sup> but only a few tiny colonies are left now. The world’s major totalitarianisms are also passé. Fascism has gone from being the preferred form of governance among half the great powers and many lesser states in the 1930s, to near extinction today. Communism has moved from being a world threat in 1950, to a mere shadow of itself at the turn of the millennium.

The major old force that remains strongly in play at the dawn of the 21st century is nationalism, particularly its violence-prone ethnonationalist variety. A good measure of the continuing power of nationalism, and of the attractiveness of the state as a form of organization and a focus of nationalist loyalty, is the number of states in existence. When the United Nations was organized after World War II, almost every nation in the world joined, for a total of 54 members. Half a century later, membership has more than tripled, and is closing in on 200.

---

<sup>48</sup>See Lenin (1916, p. 76), whose breakdown showed 90 percent of Africa under colonial control in 1900, 60 percent of Asia, all of Polynesia and Australia, and nearly a third of the Americas.

People without state status want it—and will often engage in terrorist actions to pursue it. Indeed, the majority of terrorist groups, for a long time, arose from nationalist motivations (Hoffman, 1998).<sup>49</sup>

Playing against the old, persistent, often divisive force of nationalism is the new, more unifying force of globalism. It is, to an extent, a reincarnation of the 19th century “Manchester Creed,” which held that the growth of industry and trade would create a unified, peaceful world governed by a harmony of interests (see Carr, 1939, pp. 41–62). But today’s concept of globalization has many new elements and dynamics, particularly in its deemphasis of the state and its association with the information revolution.<sup>50</sup>

Both nationalism and globalism will continue to coexist, much as the Manchester Creed coexisted with classic power politics.<sup>51</sup> Both will continue to galvanize all kinds of networks around the world. While many of the violent terrorist, criminal, and ethnic networks have mainly nationalist origins and objectives, most social networks have strong globalist dimensions. Thus, the two forces in play in today’s world—nationalism and globalism—mirror significant aspects of the two faces of netwar. This is worth pointing out, partly because many current discussions about networked actors and information-age conflict treat them as being mainly the products of globalization, and downplay the enduring significance of nationalism. However, it is important to note that some “dark netwarriors” (e.g., criminal networks) have little or no nationalist motivations.

An eventual question is whether a new “harmony of interests” based on the rise of global civil-society actors relying on soft power will erode the dominance of hard-power, nation-state politics. To some extent, developments in the theory and practice of netwar will affect both these world tendencies. That is, learning better how to build net-

<sup>49</sup>Hoffman (1998) notes that religion is also a rising force behind terrorism.

<sup>50</sup>See Held and McGrew (2000), esp. Ch. 2 (excerpted from a 1999 book by David Held, Anthony McGrew, David Goldblatt, and Jonathan Perraton), and Ch. 11 (from a 1997 paper by Michael Mann). Also see Rosenau (1990) and Nye and Donahue (2000).

<sup>51</sup>In the 19th century, the notion of a harmony of interests seemed to predominate over *realpolitik*—at least from the fall of Napoleon in 1815 to the onset of the social revolutions of 1848, and even, though falteringly, until the onset of World War I. The 20th century, on the other hand, seems to have been mainly the child of *realpolitik*.

works against crime and terror may tamp down some of the problems that attend ethno- and hypernationalism. Also, states that learn to nurture nonstate civil-society actors may help reduce some of the “demand” for terror, and some of the quests to create ever more nation states. Whichever path unfolds, it will be one in which netwar will surely be found at every turn.

The duality of Janus, first discussed in our introductory chapter, is re-introduced here. According to a modern interpretation by Arthur Koestler (1978), Janus symbolizes the eternal human tension between the need for individual self-assertion and the progress that comes with integration into larger, ultimately global groupings. When kept in equilibrium, in a system allowing individual striving but encouraging connectedness to the world as a whole, the bright face of this dual spirit moves ahead. Today, that tendency is represented by activist NGOs waging social netwar on behalf of human rights and political democracy; they aim to integrate the world around a model of civil society based on common, worldwide values. But “under unfavourable conditions, the equilibrium is upset, with dire consequences” (p. 58).<sup>52</sup> Trouble, for Koestler writing in the 1970s, arises especially when the individual is suborned in a totalitarian society—he gives the examples of Stalinist excesses, Nazi atrocities, and the infamous Milgram “authority experiments” of the 1950s. The modern-day netwar equivalent corresponds to the dark-side terrorists, criminals, and ethnonationalists who pursue self-assertion for narrow purposes.

## Two Axes of Strategy

The chapters on terrorist, criminal, and gang networks ended with observations and recommendations for strengthening counternetwar. The chapters on the social networks—Burma, Mexico, and Seattle—did not end this way, although they mentioned the countermeasures taken by the Burmese and Mexican governments and the City of Seattle. Instead, these latter case studies implied that social netwar could pressure authoritarian regimes to become democratic and impel democracies to become more responsive and transparent.

---

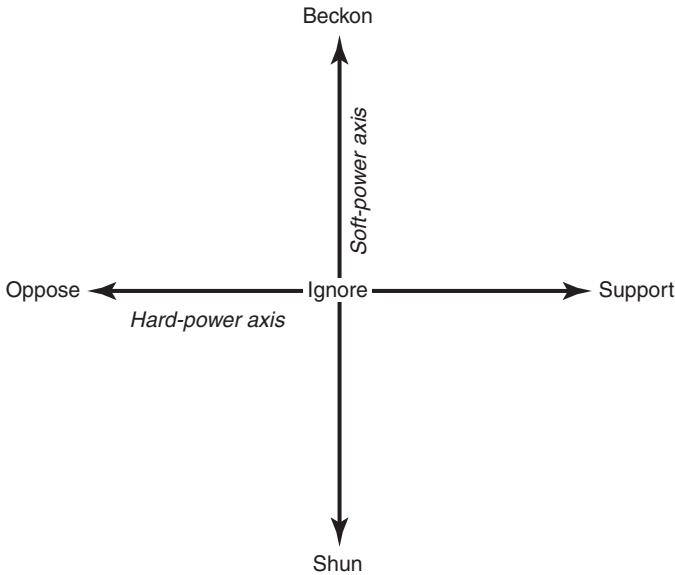
<sup>52</sup>Koestler (1978) does not adequately consider the kind of disequilibrium in which a refusal to connect with the world as a whole may lead to mischief.

In other words, netwar is not a uniformly adverse phenomenon that can, or should, always be countered. It is not necessarily a mode of conflict that always gets in the way of government aims.

States have a range of plausible strategies for dealing with networked nonstate actors. Which strategies are pursued can make a difference in whether the dark or the bright face of netwar predominates. The dark face—with its terrorists, criminals, and virulent ethnonationalists—must be countered by the United States and its allies. But, at times and in particular places, social netwar may complement a government's strategies. Who may benefit from which face depends on what government is being discussed.

In a basic sense, strategy is the methodical art of relating ends and means to deal with other actors. We view the general field of alternatives for strategists as consisting of two axes: one based on military and economic hard power, the other on idea-based soft power (see Figure 10.1). The principal axis for most strategists, and the easy one to describe, is the hard-power one—ranging from active opposition at one pole to material support at the other. In today's parlance, this axis runs from containment and deterrence at one end to engagement and partnership at the other. This axis, for example, permeates most U.S. discussions about China today.

But that is not the only axis. Strategists also think along the lines of an axis for soft-power strategies, where using military and/or economic means to oppose or support another actor is deliberately avoided. At one extreme, the soft-power axis means thoroughly shunning another actor, perhaps because of being disappointed in it, or deploring its behavior without wanting to take active measures against it, or even in the hope of arousing it to behave more positively. At the other pole, this axis consists of trying to influence an actor's behavior, rather indirectly, by holding out a set of values, norms, and standards—"dos" and "don'ts," and hopes and fears—that should determine whether or not one may end up materially favoring or opposing that actor in the future. This might be viewed as the "shining beacon on the hill" ap-



**Figure 10.1—The Two Axes of Strategy**

proach to strategy.<sup>53</sup> The midpoint of this axis—and of the hard-power axis, too—is the origin point, where no action at all is taken, perhaps because of having little or uncertain interest in an actor.

These dual axes frame the range of alternative strategies that states use in dealing with each other. Over time, the United States has used them all, often in hybrid blends. For example, during the cold war era,

<sup>53</sup>This unexpectedly paraphrases President Reagan, whose national security strategy articulated in June of 1981 called for the spread of American values, creating a new dimension of American power. He wanted to encourage the world to see, in the American example, “a shining city on a hill.” As Reagan observed in his farewell address to the nation (given January 11, 1989):

I’ve spoken of the shining city all my political life, but I don’t know if I ever quite communicated what I saw when I said it. In my mind it was a tall, proud city built on rocks stronger than oceans, windswept, God-blessed, and teeming with people of all kinds living in harmony and peace; a city with free ports that hummed with commerce and creativity (Hannaford, 1998, p. 278).



U.S. strategy revolved mainly around the hard-power axis, with emphasis on containing the Soviet Union and strengthening the NATO alliance. Lines were drawn around the world; actors were obliged to take sides. In today's loose, multipolar world, however, the soft-power axis is more in play. It is now feasible just to shun some states that once required rising degrees of containment (e.g., Cuba). Much of U.S. strategy is now more intent on using soft-power measures to exposit our standards and to attract a target (e.g., like Vietnam) into affiliation with us. Meanwhile, some states, such as Mexico and Canada, have long been subjected to a broad array of alternative strategies—depending on the times and the issues, the United States has ignored and beckoned, supported and even cautiously opposed our neighbors on occasion.

Nonstate actors of all types—especially the kinds of civil and uncivil actors analyzed in this volume—are now so powerful around the world that they cannot be dismissed by national security strategists. As strategists increasingly turn to address them, particularly the ones intent on netwar, this dual-axis perspective on strategy seems likely to frame the options usefully, with each having different implications for the future of netwar.

Each strategy has its merits, but also its costs and risks. For example, trying to stamp out criminal networks—the preferred strategy of the international community today—entails a heavy investment, including the cost involved in trying to achieve a level of cooperation among nations sufficient to deny the criminals (or terrorists, for that matter) any useful “safe havens.” Choosing this strategy presupposes that the balance of forces between states and these networks still runs heavily in favor of the former, and that firm action must be taken before criminal networks grow beyond control. For some dictatorships, of course, the target networks are not the criminal ones, but rather the local and transnational NGOs that aim to expand civil society and promote democracy.

A strategy of neglect is quite characteristic of many states' approaches to NGOs—basically ignoring them but also allowing them to grow, to engage state actors, sometimes even to pressure states into action (e.g., as in the antipersonnel landmine campaign and the effort to establish an international criminal court). This strategy holds out the

prospect of keeping the various costs of dealing with nonstate civil-society actors to a minimum, by responding to them only when necessary. It also reserves states' options, either to act directly against NGOs at some future point, or to turn to actively embrace them. A preference for this strategy may be based on an assumption that state power still dwarfs the energy and efficacy of nonstate actors; but it differs from the previous strategy in the belief that this gap in relative power seems unlikely to be narrowed anytime soon. For some states, this pattern of behavior may also apply to criminal networks in their midst.

Alternatively, states could pursue a "beacon" approach, by proclaiming standards that will determine whether active opposition or support becomes the eventual recourse. This approach holds great promise for the United States, which has often practiced it without being analytically explicit about it. It is an expression of what, in another writing, we term "noopolitik" (Arquilla and Ronfeldt, 1999). And actually it has been a regular practice of human-rights and other NGOs, more than of U.S. policymakers and strategists. George Kennan's life and work offer exemplary forms of both axes in practice—from his blueprint for active, hard-power containment during the cold war (see his famous "long telegram") to his call to rely principally on passive, soft-power ideals and values in the new era.<sup>54</sup> For an example elsewhere, one could note that Colombia's government has been resorting to aspects of this strategy—i.e., shifting from a principally hard to a soft-power approach—in its newest efforts to deal with the guerrilla organizations that control much of the national territory.

Finally, states could actively embrace and nurture favorable nonstate actors and their networks, encouraging their growth, enhancing their potency, and working with them in a coordinated manner. This may prove a boon to statecraft, when the goals of both coincide. But the risk of such a strategy is that states might unwittingly assist in the creation of a new, networked fabric of global society that may, in the end, be strong enough to constrain states when there are conflicts of inter-

---

<sup>54</sup>Kennan (1996, p. 282) puts it concisely, noting that what we call the "beacon" strategy "would be a policy that would seek the possibilities for service to morality primarily in our own behavior, not in our judgment of others."

est. This may well be an acceptable risk; but it is one that has to be thoroughly assessed.<sup>55</sup> As we look around the world today, we see little sustained embrace of networks of civil-society actors, and only faint hints that some states may be reaching out to transnational criminal and terror networks.<sup>56</sup>

Individual state strategies toward nonstate networks have in practice tended to feature some mixing and blending of these approaches. The United States, in particular, has pursued confrontation against criminal and terror networks, while trying to ignore NGOs when their aims conflict with government policy (e.g., as in the anti-landmine movement and the international criminal court initiative). With regard to the Intifadah waged by the Palestinians, American strategy can be characterized as active support for the “rights” of the Palestinians (not to mention Israeli rights), mixed with “shunning” those who are associated with violent acts—on both sides.

Much more can and should be done to shift to a strategy of both cultivating and cooperating with NGOs. Since U.S. policymakers have tended to emphasize the threats posed by emerging nonstate ac-

---

<sup>55</sup>We have related in other writings (e.g., Arquilla and Ronfeldt, 1999) our own view that states will remain the paramount actors in the international system. As a result of the information revolution, nonstate actors will continue to gain strength and influence; and this will lead to changes in the nature of the state—but not its “withering away.” What will occur is a transformation, where some states will emerge stronger than ever because of a capacity to work conjointly with NGOs and other civil nonstate actors. As this process unfolds, there will be a rebalancing of relations among state, market, and civil-society actors around the world—in ways that favor “noopolitik” over realpolitik.

<sup>56</sup>For example, Afghanistan’s Taliban government, while it refuses to extradite Osama bin Laden, shows little sign of protecting him out of self-interest. Rather, its position seems to stem from a sense of obligation to a heroic fighter in the war against the Soviet occupation of Afghanistan in the 1980s. In Colombia, far from embracing criminal networks, the government is imperiled by them. The only unambiguously clear example of a state reaching out to a nonstate organization thought to engage in terrorist attacks is that of Iran and Hizbollah, which operates out of southern Lebanon and recently drove the Israeli Defense Forces out of Lebanon, after two decades of occupation. Finally, there are some signs that China is cooperating on some levels with certain criminal networks—modern-day pirates in particular—but the evidence is scant at best.

tors,<sup>57</sup> it is not hard to see how the potential opportunities of engaging and helping to build a global civil society may have been overlooked so far. But the cost of inattention to this issue is already substantial (e.g., political opprobrium suffered because of lack of U.S. support for the antipersonnel landmine ban), and will grow.

Learning not only to live but also to work with NGOs to create new governance schemes for addressing social problems is becoming the cutting edge of policy and strategy.<sup>58</sup> It would seem advisable for the United States to take the lead at this—possibly in connection with newly emerging concepts about “information engagement.” However, the states that may be more willing to engage NGOs may well be the ones that possess less hard power and are less interested in competitive realpolitik. Sweden, a good friend to nonstate actors, has not been in a shooting war for 200 years. So perhaps the “beaconing” and nurturing strategies toward nonstate actors that we have articulated will have to diffuse from the periphery of the world political system to its core actors—slowly and over time—if the greater powers cannot advance the process themselves.

This concluding discussion could no doubt be made more thorough and nuanced. But, brief and selective as it is, it serves to underscore what we think is the important point: The rise of netwar and its many early successes imply the need for statecraft to adjust to—perhaps be transformed by—these civil and uncivil manifestations of the information revolution. Most central concepts about national security are over half a century old now. Containment, mutual deterrence, coercive diplomacy, all seem ever less relevant to the types of challenges confronting nation states. Netwar—with its emphasis on empowering

---

<sup>57</sup>See the discussion above about the recently released *Global Trends 2015* report (National Intelligence Council, 2000) which focuses to a large extent on the rise of networked criminal and terrorist organizations, while spending very little time on the opportunities that may arise from working with and supporting nonstate civil-society actors.

<sup>58</sup>A growing literature has begun to identify lessons and options for states and NGOs to work together. Recent sources we consulted include Florini (2000), Reinicke (1999–2000), Gerlach, Palmer, and Stringer (2000), and Simmons (1998); Fukuyama and Wagner (2000) for a RAND research perspective; Chayes, Chayes, and Raach (1997) on conflict management situations; Metzl (1996) and Tuijl (1999) on human rights issues; and Carothers (1999–2000) and Clark, Friedman, and Hochstetler (1998) for cautionary observations about expecting too much from global civil society.

dispersed small groups, its reliance on the power of the story, and its suitability to leaderless networks adept at swarming—should call forth a strategic renaissance among those who would either employ it or oppose it. This conceptual rebirth, if allowed to thrive, will undoubtedly take us all far from the old paradigms. Deterrence and coercion will not disappear entirely as tools of statecraft; but, more and more often, suasion will have to be tried, as our understanding of the limited usefulness of force grows ever clearer.

## BIBLIOGRAPHY

- Arquilla, John, and David Ronfeldt, *The Advent of Netwar*, Santa Monica, Calif.: RAND, MR-789-OSD, 1996.
- Arquilla, John, and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica, Calif.: RAND, MR-1033-OSD, 1999.
- Arquilla, John, and David Ronfeldt, *Swarming and the Future of Conflict*, Santa Monica, Calif.: RAND, DB-311-OSD, 2000.
- Arquilla, John, and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997.
- Barkun, Michael, *Religion and the Racist Right: The Origins of the Christian Identity Movement*, Revised edition, Chapel Hill, N.C.: University of North Carolina Press, 1997.
- Beam, Louis, "Leaderless Resistance," *The Seditiousist*, Issue 12, February 1992 (text can sometimes be located at [www.louisbeam.com/leaderless.htm](http://www.louisbeam.com/leaderless.htm)).
- Bertalanffy, Ludwig von, *General Systems Theory: Foundations, Development, Applications* (revised edition), New York: George Braziller, 1968.
- Brin, David, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, Mass.: Addison-Wesley, 1998.

- Brown, John Seely, and Paul Duguid, *The Social Life of Information*, Boston: Harvard Business School Press, 2000.
- Burghardt, Tom, *Leaderless Resistance and the Oklahoma City Bombing*, San Francisco: Bay Area Coalition for Our Reproductive Rights (BACORR), April 1995a.
- Burghardt, Tom, *Dialectics of Terror: A National Directory of the Direct Action Anti-Abortion Movement and Their Allies*, San Francisco: Bay Area Coalition for Our Reproductive Rights (BACORR), October 1995b.
- Burns, Tom, and G. M. Stalker, *The Management of Innovation*, London: Tavistock, 1961.
- Burt, Ronald S., *Structural Holes: The Social Structure of Competition*, Cambridge, Mass.: Harvard University Press, 1992.
- Capra, Fritjof, *The Web of Life: A New Scientific Understanding of Living Systems*, New York: Anchor Books, 1996.
- Carothers, Thomas, "Civil Society," *Foreign Policy*, No. 117, Winter 1999–2000, pp. 18–29.
- Carr, Edward Hallett, *The Twenty Years' Crisis, 1919–1939*, London: Macmillan, 1939.
- Castells, Manuel, *The Information Age: Economy, Society and Culture*, Vol. I, *The Rise of the Network Society*, Malden, Mass.: Blackwell Publishers, 1996.
- Castells, Manuel, *The Information Age: Economy, Society and Culture*, Vol. III, *End of the Millennium*, Malden, Mass.: Blackwell Publishers, 1998.
- Cebrowski, Vice Admiral Arthur, and John Garstka, "Network-Centric Warfare," *Proceedings of the United States Naval Institute*, Vol. 24, No. 1, January 1998, pp. 28–35.
- Chayes, Antonia Handler, Abram Chayes, and George Raach, "Beyond Reform: Restructuring for More Effective Conflict Intervention," *Global Governance*, Vol. 3, No. 2, May–August 1997, pp. 117–145.

- Clark, Ann Marie, Elisabeth J. Friedman, and Kathryn Hochstetler, "The Sovereign Limits of Global Civil Society: A Comparison of NGO Participation in UN World Conferences on the Environment, Human Rights, and Women," *World Politics*, Vol. 51, No. 1, October 1998, pp. 1–35.
- Cohen, Roger, "Who Really Brought Down Milosevic," *The New York Times Magazine*, November 26, 2000, pp. 43–47, 118, 148.
- Copeland, Thomas E., ed., *The Information Revolution and National Security*, Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, 2000.
- Coyne, Kevin P., and Renée Dye, "The Competitive Dynamics of Network-Based Businesses," *Harvard Business Review*, January–February 1998, pp. 99–109.
- Dertouzos, Michael, *What Will Be: How the New World of Information Will Change Our Lives*, San Francisco: HarperCollins, 1997.
- DeSanctis, Gerardine, and Janet Fulk, eds., *Shaping Organizational Form: Communication, Connection, and Community*, Thousand Oaks, Calif.: Sage Publications, 1999.
- Evan, William M., "An Organization-Set Model of Interorganizational Relations," in Matthew Tuite, Roger Chisholm, and Michael Radnor, eds., *Interorganizational Decisionmaking*, Chicago: Aldine Publishing Company, 1972, pp. 181–200.
- Evans, Philip B., and Thomas S. Wurster, "Strategy and the New Economics of Information," *Harvard Business Review*, September–October 1997, pp. 71–82.
- Florini, Ann, "The End of Secrecy," *Foreign Policy*, No. 111, Summer 1998, pp. 50–63.
- Florini, Ann M., ed., *The Third Force: The Rise of Transnational Civil Society*, Washington, D.C.: Carnegie Endowment for International Peace, 2000.
- Freeman, Linton C., "Visualizing Social Networks," *Journal of Social Structure*, Vol. 1, No. 1, February 4, 2000, available only online, [www.heinz.cmu.edu/project/INSNA/joss/vsn.html](http://www.heinz.cmu.edu/project/INSNA/joss/vsn.html).

Fukuyama, Frank, *The Great Disruption: Human Nature and the Reconstitution of Social Order*, New York: The Free Press, 1999.

Fukuyama, Frank, and Caroline S. Wagner, *Information and Biological Revolutions: Global Governance Challenges—Summary of a Study Group*, Santa Monica, Calif.: RAND, MR-1139-DARPA, 2000.

Gerlach, Luther, "The Structure of Social Movements: Environmental Activism and Its Opponents," in Jo Freeman and Victoria Johnson, eds., *Waves of Protest: Social Movements Since the Sixties*, Lanham, Mass.: Rowman and Littlefield, 1999, pp. 85–98.

Gerlach, L. P., G. B. Palmer, and Tish Stringer, *Managing Global Change Through Segmentary and Polycentric Networks*, paper presented at the annual meeting of the American Anthropology Association, San Francisco, November 14, 2000, posted at [www.unlv.edu/faculty/gbp/gerlach/managing2.htm](http://www.unlv.edu/faculty/gbp/gerlach/managing2.htm).

Gowing, Nik, *New Challenges and Problems for Information Management in Complex Emergencies: Ominous Lessons from the Great Lakes and Eastern Zaire in Late 1996 and Early 1997*, paper prepared for a conference on Dispatches from Disaster Zones: The Reporting of Humanitarian Enterprises, London, May 27, 1998.

Granovetter, Mark, "The Strength of Weak Ties," *American Journal of Sociology*, Vol. 78, No. 6, May 1973, pp. 1360–1380.

Granovetter, Mark S., "Economic Action and Social Structure: The Problem of Embeddedness," *American Journal of Sociology*, Vol. 91, No. 3, November 1985, pp. 481–510.

Haas, Peter M., "Introduction: Epistemic Communities and International Policy Coordination," *International Organization*, Vol. 46, No. 1, Winter 1992, pp. 1–36.

Hannaford, Peter, *The Quotable Ronald Reagan*, Washington, D.C.: Regnery Publishing, Inc., 1998.

Held, David, and Anthony McGrew, eds., *The Global Transformations Reader: An Introduction to the Globalization Debate*, Malden, Mass.: Polity Press, Blackwell Publishers, 2000.

Hoffman, Bruce, *Inside Terrorism*, New York: Columbia University Press, 1998.



Jacques, Elliot, "In Praise of Hierarchy," *Harvard Business Review*, January–February 1990, pp. 127–133.

Keck, Margaret E., and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics*, Ithaca: Cornell University Press, 1998.

Kelly, Kevin, *Out of Control: The Rise of Neo-Biological Civilization*, New York: A William Patrick Book, Addison-Wesley Publishing Company, 1994.

Kennan, George, *At a Century's Ending*, New York: Morrow, 1996.

Koestler, Arthur, *Janus*, New York: Random House, 1978.

Kumar, Kuldeep, and Han G. van Dissel, "Sustainable Collaboration: Managing Conflict and Cooperation in Interorganizational Systems," *MIS Quarterly*, September 1996, pp. 279–300.

Kumon, Shumpei, "Japan as a Network Society," in Shumpei Kumon and Henry Rosovsky, eds., *The Political Economy of Japan*, Vol. 3, *Cultural and Social Dynamics*, Stanford, Calif.: Stanford University Press, 1992, pp. 109–141.

La Porte, Todd R., ed., *Organized Social Complexity: Challenge to Politics and Policy*, Princeton, N.J.: Princeton University Press, 1975.

Lenin, V. I., *Imperialism. The Highest Stage of Capitalism*, New York: International Publishers, [1916] 1939.

Libicki, Martin, "Rethinking War: The Mouse's New Roar?" *Foreign Policy*, No. 117, Winter 1999–2000, pp. 30–43.

Lipnack, Jessica, and Jeffrey Stamps, *The Age of the Network*, New York: Wiley & Sons, 1994.

Metzl, Jamie Frederic, "Popular Diplomacy," *Daedalus*, Vol. 128, No. 2, Spring 1999, pp. 177–192.

Metzl, Jamie F., "Information Technology and Human Rights," *Human Rights Quarterly*, Vol. 18, No. 4, November 1996, pp. 705–746.

Miles, Raymond E., and Charles C. Snow, "Organizations: New Concepts for New Forms," *California Management Review*, Vol. 28, No. 3, Spring 1986, pp. 62–73.

Miles, Raymond E., and Charles C. Snow, "Causes of Failure in Network Organizations," *California Management Review*, Summer 1992, pp. 53–72.

Mintzberg, Henry, "Organizational Design: Fashion or Fit?" *Harvard Business Review*, January–February 1981.

Monge, Peter R., and Noshir S. Contractor, "Emergence of Communication Networks," in F. M. Jablin and L. L. Putnam, eds., *The New Handbook of Organizational Communication: Advances in Theory, Research, and Methods*, Thousand Oaks, Calif.: Sage, 2001, pp. 440–502.

Monge, Peter, and Janet Fulk, "Communication Technology for Global Network Organizations" in Gerardine DeSanctis and Janet Fulk, eds., *Shaping Organizational Form: Communication, Connection, and Community*, Thousand Oaks, Calif.: Sage Publications, 1999, pp. 71–100.

Nohria, Nitin, and Robert G. Eccles, eds., *Networks and Organizations: Structure, Form, and Action*, Boston: Harvard Business School Press, 1992.

Nye, Joseph S., and John D. Donahue, eds., *Governance in a Globalizing World*, Washington, D.C.: Brookings Institution Press, 2000.

Pagels, Heinz R., *The Dreams of Reason: The Computer and the Rise of the Sciences of Complexity*, New York: Bantam Books, 1989 (originally, Simon & Schuster, 1988).

Perrow, Charles, *Complex Organizations: A Critical Essay*, 2nd edition, Glenview, Ill.: Scott, Foresman and Company, 1979.

Perrow, Charles, "Small Firm Networks, in Nitin Nohria and Robert G. Eccles, eds., *Networks and Organizations: Structure, Form, and Action*, Boston: Harvard Business School Press, 1992, pp. 445–470.

Powell, Walter W., "Neither Market Nor Hierarchy: Network Forms of Organization," in Barry M. Staw and L. L. Cummings (ed.), *Research in Organizational Behavior: An Annual Series of Analytical Essays and Critical Reviews*, Vol. 12, Greenwich, Conn.: JAI Press Inc., 1990, pp. 295–336.

Reinicke, Wolfgang H., "The Other World Wide Web: Global Public Policy Networks," *Foreign Policy*, No. 117, Winter 1999–2000, pp. 44–57.

Risse, Thomas, "'Lets Argue!'—Communicative Action in World Politics," *International Organization*, Vol. 54, No. 1, Winter 2000, pp. 1–39.

Ronfeldt, David, "Cyberocracy Is Coming," *The Information Society*, Vol. 8, No. 4, 1992, pp. 243–296.

Ronfeldt, David, *Tribes, Institutions, Markets, Networks—A Framework About Societal Evolution*, Santa Monica, Calif.: RAND, P-7967, 1996.

Ronfeldt, David, "Social Science at 190 MPH on NASCAR's Biggest Superspeedways," *First Monday*, Feb 2000, [http://firstmonday.org/issues/issue5\\_2/index.html](http://firstmonday.org/issues/issue5_2/index.html).

Ronfeldt, David, and John Arquilla, "From Cyberspace to the Noosphere: Emergence of the Global Mind," *New Perspectives Quarterly*, Vol. 17, No. 1, Winter 2000, pp. 18–25.

Rosenau, James N., *Turbulence in World Politics: A Theory of Change and Continuity*, Princeton, N.J.: Princeton University Press, 1990.

Rothkopf, David J., "The Disinformation Age," *Foreign Policy*, No. 114, Spring 1999, pp. 83–96.

Rutherford, Ken, *The Landmine Ban and NGOs: The Role of Communications Technologies*, draft paper presented at a conference sponsored by The Nautilus Institute, San Francisco, December 1999, [www.nautilus.org/info-policy/workshop/papers/rutherford.html](http://www.nautilus.org/info-policy/workshop/papers/rutherford.html).

Schein, Edgar, *Organizational Culture and Leadership*, Oxford: Jossey-Bass, 1985.

Schweizer, Peter, *Victory: The Reagan Administration's Secret Strategy That Hastened the Collapse of the Soviet Union*, New York: The Atlantic Monthly Press, 1994.

Shafritz, Jay M., and J. Steven Ott, *Classics of Organization Theory*, 4th edition, New York: Harcourt Brace, 1996.

Shaw, Marvin, *Group Dynamics: The Psychology of Small Group Behavior*, 2nd edition, New York: McGraw-Hill Book Company, 1976.

Simmons, P. J., "Learning to Live with NGOs," *Foreign Policy*, No. 112, Fall 1998, pp. 82–96.

Simon, Herbert A., "The Architecture of Complexity," (1962), in Herbert A. Simon, *The Sciences of the Artificial*, Cambridge, Mass.: The M.I.T. Press, 1969.

Stern, Kenneth, *A Force upon the Plain: The American Militia Movement and the Politics of Hate*, New York: Simon & Schuster, 1996.

Strogatz, Steven H., "Exploring Complex Networks," *Nature*, Vol. 410, March 8, 2001, pp. 268–276.

Tuijl, Peter van, "NGOS and Human Rights: Sources of Justice and Democracy," *Journal of International Affairs*, Vol. 52, No. 2, Spring 1999, pp. 493–512.

Wasserman, S., and K. Faust, *Social Network Analysis: Methods and Applications*, Cambridge, Mass.: Cambridge University Press, 1994.

Watts, Duncan J., *Small Worlds: The Dynamics of Networks Between Order and Randomness*, Princeton, N.J.: Princeton University Press, 1999.

Wellman, Barry, and S. D. Berkowitz, *Social Structures: A Network Approach* (updated edition), Greenwich, Conn.: JAI Press, 1997.

Williams, Jody, and Stephen Goose, "The International Campaign to Ban Landmines," in Maxwell A. Cameron, Robert J. Lawson, and Brian W. Tomlin, eds., *To Walk Without Fear: The Global Movement to Ban Landmines*, New York: Oxford University Press, 1998, pp. 20–47.

Woodward, Robert, *Veil: The Secret Wars of the CIA, 1981–1987*, New York: Simon and Schuster, 1987.

Wray, Stefan, *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics*, paper for a conference on The World Wide Web and Contemporary Cultural Theory, Drake University (Des Moines, Ia.), November 1998, [www.nyu.edu/projects/wray/wwwhack.html](http://www.nyu.edu/projects/wray/wwwhack.html).